A35697 065855.0199

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

On Appeal to the Board of Appeals and Interferences

Appellants	:	Edward J. Hogan et al.		
Serial No.	:	09/833,049	Examiner :	Firmin Backer
Filed	:	April 11, 2001	Group Art Unit:	3621

For : METHOD AND SYSTEM FOR CONDUCTING SECURE PAYMENTS OVER A COMPUTER NETWORK

APPEAL BRIEF

I hereby certify that this paper addressed to: Commissioner for Patents, P.O. Box 1450, Arlington, VA 22313-1450 is being transmitted to the United States Patent and Trademark Office via EFS on the date indicated below:

May 17, 2007
Date of Deposit

Manu J Tejwani	37,952
Attorney Name	Registration No.
Signature	May 17, 2007
	Date of Signature

TABLE OF CONTENTS

A35697 -65855.0199

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

On Appeal to the Board of
Appeals and Interferences

Appellants	:	Edward J. Hogan et al.		
Serial No.	:	09/833,049	Examiner :	Firmin Backer
Filed	:	April 11, 2001	Group Art Unit:	3621

For : METHOD AND SYSTEM FOR CONDUCTING SECURE PAYMENTS OVER A COMPUTER NETWORK

APPEAL BRIEF

Commissioner for Patents
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellants have on even date filed a Notice of Appeal from the final rejection of more-than-twice rejected claims 1-5 and 7-16 contained in an Office Action dated November 17, 2007. The rejection was maintained in an Advisory Action dated April 5, 2007.

Appellants hereby timely submit, pursuant to 37 C.F.R. § 41.37, an Appeal Brief in support of the appeal of the rejection of pending claims 1-5 and 7-16.

I. REAL PARTY IN INTEREST

The real party in interest is MasterCard International Incorporated, 2000 Purchase Street, Purchase, New York 10577-2509 ("MasterCard"). The real party in interest is MasterCard International Incorporated, 2000 Purchase Street, Purchase, New York 10577-2509 ("MasterCard"). MasterCard is the assignee of the entire right, title, and interest in the present application by virtue of an Assignment, which is dated November 27, 2000 and December 4, 2000, and which was recorded on February 1, 2001 at Reel 011500 Frame 0741.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 1-5 and 7-16 are pending. Claim 6 is cancelled. Claim 17 was previously withdrawn from consideration in response to a restriction requirement.

Claims 1-5 and 7-16 stand finally rejected under 35 U.S.C. § 102(e) allegedly as being anticipated by Breck et al. U.S. patent application Publication No. 2004/0210449 ("Breck"). Claim 1 also stand rejected under 35 U.S.C. § 112, second paragraph, allegedly as being indefinite.

An Advisory Action dated April 5, 2007 maintains the rejection of the claims.

IV. STATUS OF AMENDMENTS

In a Reply dated February 20, 2007, appellants traversed, but proposed an amendment to claim 1 to address the § 112 indefiniteness rejection.

Entry of amended claim 1 was refused by the Advisory Action dated April 5, 2007.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention described in the above-identified application relates to transmitting payments securely over a computer network, such as the Internet, and transmitting sensitive information securely over public communication channels.

In particular, appellants' invention relates to systems and methods for authorizing on-line payment transactions between a merchant and a customer, in a manner in which the customer's payment account number is secured by encryption. The payment account number is encrypted in manner, which preserves payment account number privacy, but allows the proper customer payment account to used for routing the payment authorization request from the merchant to the proper bank (e.g., customer's payment card issuer) for authorization and conversely allows the bank's response to be routed to the proper merchant.

Certain embodiments of the invention (e.g., claims 5, 9 and 14) require computer generation of a message or transaction authentication code, which is positioned in the discretionary data field of a standard payment card track image and then transmitted over the electronic payment network.

Claim 1 reads:

A method of conducting a transaction using a payment account for payment over a payment network, [*See Specification page 4 ¶[0010], paragraph lines 1-2*] the method comprising:

(a) receiving by a service provider other than an issuer of the payment account a first authorization request for the authorization of the transaction using a first payment account number [*See Specification page 4 ¶[0010], paragraph lines 1-2, FIG. 3*], wherein:

(i) the first payment account number has a service provider identification number that is associated with the service provider other than the issuer [*See Specification page 4 ¶[0010], paragraph lines 5-6, page 14 ¶[0046], paragraph lines 2-4,*] and is associated with a second payment account number that has an issuer identification number associated with the issuer [*See e.g., Specification page 4 ¶[0010], paragraph lines 6-8, page 14 ¶[0049], paragraph lines 1-4, etc.*], said second payment account number not being included in said first authorization request [*See Specification page 4 ¶[0010], paragraph lines 6-8, page 14 ¶[0049], paragraph lines 1-4, etc.*];

(ii) the first authorization request includes a first acquirer code associated with an acquirer [*See Specification page 4 ¶[0010], paragraph lines 9-10, page 15 ¶[0051], paragraph lines 1-5*]; and

(iii) the first authorization request is routable through the payment network to the service provider based on said service provider identification number [*See Specification page 4 ¶[0010], paragraph lines 11-13, FIG. 3*];

(b) responsive to the first authorization request, transmitting by the service provider a second authorization request for authorization of the transaction using the second payment account number [*See Specification page 4 ¶[0011], paragraph lines 1-5, pages 16-1, ¶[0055], paragraph lines 1-5*], the second authorization request including a second acquirer code

associated with the service provider and being routable through the payment network to the issuer based on said issuer identification number [*See e.g., Specification page 4 ¶[0011], paragraph lines 1-5, pages 16-1, ¶[0055], paragraph lines 1-5, FIG. 3*].

(c) receiving from the issuer a response to the second authorization request transmitted by the service provider, the response including the second acquirer code and being routable through the payment network based on that code [*See e.g., Specification pages 4 -5 ¶[0012], paragraph lines 1-3, FIG. 4*]; and

(d) transmitting from the service-provider to the acquirer a response to the first authorization request received by the service provider based on the response to the second authorization request received by the service-provider from the issuer, the response to the first authorization request including the first acquirer code and being routable through the payment network based on that code [*See e.g., Specification pages 4 -5 ¶[0012], paragraph lines 3-6, FIG. 5*].

Claim 5 reads:

5. A method of conducting a transaction with a merchant over a communications network using a first payment account number that is associated with a second payment account number [*See e.g., Specification pages 4 -5 ¶[0012], paragraph lines 3-6, FIG. 5*], the method comprising:

(a) generating a message authentication code based on one or more transaction details [*See e.g. Specification pages 11-12 ¶[0036], paragraph lines 1-14*];

(b) transmitting at least the first payment account number and the message authentication code to the merchant [*See e.g. Specification page 13 ¶[0040], paragraph lines 1-6, ¶[0041, paragraph lines 1-3*];

(c) requesting by the merchant a first authorization request for payment of the transaction using the first payment account number [*See e.g. Specification page 13 ¶[0042], paragraph lines 1-4, FIG. 3*], said second payment account number not being included in said first authorization request [*See e.g. Specification page 13 ¶[0040], paragraph lines 1-3*], the request being formatted as if payment were tendered at a point-of-sale terminal with a conventional magnetic-stripe payment card, the format having a track with at least a discretionary data field and said message authentication code being transmitted in said discretionary data field [*See e.g. Specification page 13 ¶[0042], paragraph lines 1-4, [0038], paragraph lines 1-2*];

(d) responsive to the authorization request for the first payment account number, requesting an authorization for payment of the transaction using the second payment account number [*See e.g., Specification page 4 ¶[0011], paragraph lines 1-5, pages 16-17, ¶[0055], paragraph lines 1-5, etc.*]; and

(e) accepting or declining the authorization request for the first payment account number based on the response to the authorization request for the second payment account number and the message authentication code [*See e.g., Specification page 15 ¶[0011], paragraph lines 1-6, page 18, ¶[006], paragraph lines 1-8, etc/*],

wherein said first and second payment account numbers include respective service provider and issuer identification numbers, wherein a service provider other than the issuer receives said

merchant's request through a payment network based on said service provider identification number, and wherein said service provider generates said request for authorization of payment using the second payment account number and routes said request to said issuer through said network based on said issuer identification number [*See e.g., FIGS 3-5*].

Claim 9 reads:

9. A method of conducting a transaction over a communications network, the method comprising:

issuing by an issuer having an issuer identification number a first payment account number to a user having a computer [*See e.g. Specification FIG. 1,*], said issuer identification number being associated with said first payment account number;

providing a security module for generating a secret key unique to each first account number issued [*See e.g. Specification FIG. 1, pages 9-10¶[0030], paragraph lines 1-8, etc.]*],;

generating a second account number associated with said first payment account number [*See e.g. Specification FIG. 1, pages 7-8, ¶[0007] paragraph lines 69 and 19-20, etc.*];

providing a secure payment application by a service provider to said computer, said application comprising said second account number and said secret key [*See e.g. Specification, page 7, ¶[0007] paragraph lines 1-3, etc.*];

storing said secure payment application on said computer[*See e.g. Specification, page 97, ¶[0028] paragraph lines 1-3, etc.*];

selecting a merchant with whom to conduct said financial transaction, said merchant having an associated acquirer code [*See e.g. Specification, FIG. 2, page 11 ¶[0033] lines 1-3, etc.*];

passing to said computer transaction data [*See e.g. Specification, page 11 ¶[0035] lines 1-4, etc.*];

computer generating a message authentication code based on said transaction data [*See e.g. Specification, page 11 ¶[0036] lines 1-3, etc.*];

transmitting track data in standard track image format to said merchant [*See e.g. Specification, page 12 ¶[0037] lines 1-5, etc.*], said track data comprising said computer generated message authentication code and said second account number [*See e.g. Specification, page 12 ¶[0038] lines 1-4, etc.*], wherein said computer generated message authentication code is directly positioned in the discretionary data field of the standard track image format [*See e.g. Specification, page 121 ¶[0038] lines 1-4, etc.*],;

generating a first authorization request based on said data [*See e.g. Specification, page 13 ¶[0038] lines 1-4, etc.*],;

transmitting said first request to said service provider [*See e.g. Specification, FIG. 3, etc.*];

verifying said first request with said secret key [*See e.g. Specification, page 16 ¶[0055] lines 1-2 etc.*];

obtaining said first payment account number associated with said second account number [*See e.g. Specification, page 15 ¶[0049] paragraph lines 1-4, etc.*];;

transmitting a second authorization request using said first payment account number to said issuer identification number associated with said first payment account number [*See e.g. Specification, pages 16-17 ¶[0055] paragraph lines 1-6, etc.*]; and

authorizing or rejecting said second request [*See e.g. Specification, page 18 ¶[0059] paragraph lines 1-4, etc.*].

Claim 14 reads:

14. A method of conducting a transaction involving a merchant over an electronic payment network, the method comprising:

receiving data related to said transaction from said merchant [*See e.g. Specification, FIGS. 2-3, etc.*];

computing a message authentication code based on said data related to said transaction [*See e.g. Specification, pages 11-12 ¶[0036] paragraph lines 1-3 and 7-14, etc.*];;

placing said message authentication code in a portion of the discretionary data field of a standard payment card magnetic stripe track format to form a track image [*See e.g. Specification, page 12 ¶[0038] paragraph lines 1-4, etc.*];; and

transmitting said track image, including said message authentication code, over said payment network, [*See e.g. Specification FIGS. 2-3, etc.*];.

without first storing said message authentication code on a magnetic stripe of a payment card [*See e.g. Specification, page 12 ¶[0037] paragraph lines 1-5, etc.*].

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The rejection of claims 1-5 and 7-16 under 35 U.S.C. § 102(e) allegedly as being anticipated by Breck et al. U.S. patent application Publication No. 2004/0210449 ("Breck"), and the rejection of claim 1 under 35 U.S.C. § 112, second paragraph, allegedly as being indefinite.

VII. ARGUMENT

The Examiner's has improperly rejected claims 1-5 and 7-16 under 35 U.S.C. § 102(e) as being anticipated by Breck et al. U.S. patent application Publication No. 2004/0210449 ("Breck"), and has improperly rejected claim 1 under 35 U.S.C. § 112, second paragraph, as being indefinite. The Examiner's rejections are incorrect and should be reversed.

35 U.S.C. § 112, second paragraph, rejection of claim 1

Appellants submit the phrase "that code" is clear and definite manner in each instance of its recitation in claim 1 (i.e., in clauses (c) and (d) of the claim 1). In each instance, "that" code is readily understood in common grammatical usage as referring to the preceding named code in the same clause.

For example, in claim 1 clause (c): "receiving from the issuer a response to the second authorization request transmitted by the service provider, the response including *the second acquirer code* and being routable through the payment network based on *that code*," the latter usage of "that code" clearly and definitely refers to the preceding "*second acquirer code*."

Further, in claim 1 clause (d): "transmitting from the service-provider to the acquirer a response to the first authorization request received by the service provider based on the response to the second authorization request received by the service-provider from the issuer, the response to the first authorization request including *the first acquirer code* and being routable through the payment network based on *that code,"* the latter usage of "that code" clearly and definitely refers to the preceding "*first acquirer code*."

Accordingly, claim 1 is clear and definite, and conforms to all requirements of 35 U.S.C. § 112, second paragraph.

Accordingly, the § 112 indefiniteness rejection of claim 1 should be reversed.

35 U.S.C. § 102(e) anticipation rejection

Appellants' invention provides methods and systems for authorizing on-line payment transactions between a merchant and a customer, in a manner in which the customer's payment account number is secured by encryption. The payment account number is encrypted in manner, which preserves payment account number privacy, but allows the proper customer payment account to used for routing the payment authorization request from the merchant to the proper bank (e.g., customer's payment card issuer) for authorization and conversely allows the bank's response to be routed to the proper merchant.

Appellants note that cited reference —Breck, is unrelated to subject matter of appellants' claims. Breck relates to the use of a "dummy" or "proxy" number (i.e., Secure transaction number (STN) 15) in lieu of a cardholder's actual or primary account number (PAN) for payment transaction processing, which involves a card holder, a merchant and an issuer (card provider). (See Breck, FIGS. 1 and 8, ¶¶ [0048], [0052], [0053], [0054], [0058], [0059], [0066], [0074], [0076]-[0083], and [0090]). In Breck, the payment processing between the merchant and the issuer/card provider (i.e., step 115, FIGS. 1 and 8) is conventional except for the replacement of the PAN by the dummy STN 15. (See e.g., Breck ¶[0054], and ¶[0081]): "the merchant 2 submits an authorization request to the card provider 3, as it would with any other credit card transaction").

Breck does not relate to, and fails to show appellants' inventive modifications and improvements over conventional payment processing (e.g., authorization request processing) between merchant and issuer.

To anticipate the claims as alleged by the Examiner, Breck must teach each element of the claims. (See MPEP § 2121: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) and "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)).

Appellants submit that Breck does not teach each respective element of claims 1-5 and 7-16, and therefore does not anticipate any of these claims.

Claims 1-4

The elements of claim 1 include:

(a) receiving by a service provider other than an issuer of the payment account a first authorization request for the authorization of the transaction using a first payment account number, wherein:

(i) the first payment account number has a service provider identification number that is associated with the service provider other than the issuer and is associated with a second payment account number that has an issuer identification number associated with the issuer, said second payment account number not being included in said first authorization request;

(ii) ...

(iii) the first authorization request is routable through the payment network to the service provider based on said service provider identification number;

(b) responsive to the first authorization request, transmitting by the service provider a second authorization request for authorization of the transaction using the second payment account number, the second authorization request including a second acquirer code associated with the service provider and being routable through the payment network to the issuer based on said issuer identification number;

(c) receiving from the issuer a response to the second authorization request transmitted by the service provider, the response including the second acquirer code and being routable through the payment network based on that code; and

(d) transmitting from the service provider to the acquirer a response to the first authorization request received by the service provider based on the response to the second authorization request received by the service provider from the issuer, the response to the first authorization request including the first acquirer code and being routable through the payment network based on that code.

Contrary to the assertion in the Office Action (Office Action pages 3-4, § 7), Breck does not teach about the use of two different payment account numbers or a service provider's involvement in a hyphenated transaction processing between merchant, service provider and the issuer in the manner of appellants' claim 1.

In particular, Breck does not show "a first payment account number [that] has a service provider identification number that is associated with the service provider [and] a second payment account number that has an issuer identification number associated with the issuer, said second payment account number not being included in said first authorization request."

Further, Breck does not mention or suggest a service provider, an acquiring bank or any other intermediate entity, which sends a second authorization request that according to claim 1 has a "second identification number associated with the issuer" and "a second payment account number [that is] not [] included in the first authorization request."

For at least the foregoing reasons, claim 1 and its dependent claims 2-4 are not anticipated by and are patentable over Breck.

Accordingly, the anticipation rejection of these claims should be reversed.

Claims 5, 7 and 8

The elements of claim 5 include:

(a) generating a message authentication code based on one or more transaction details;

(b) transmitting at least the first payment account number and the message authentication code to the merchant;

(c) requesting by the merchant an a first authorization request for payment of the transaction using the first payment account number, said second payment account number not being included in said first authorization request, the request being formatted as if payment were tendered at a point-of-sale terminal with a conventional magnetic-stripe payment card, the format having a track with at least a discretionary data field and said message authentication code being transmitted in said discretionary data field;

(d) responsive to the authorization request for the first payment account number, requesting an authorization for payment of the transaction using the second payment account number; and

(e) accepting or declining the authorization request for the first payment account number based on the response to the authorization request for the second payment account number and the message authentication code,

wherein said first and second payment account numbers include respective service provider and issuer identification numbers, wherein a service provider other than the issuer receives said merchant's request through a payment network based on said service provider identification number, and wherein said service provider generates said request for authorization of payment using the second payment account number and routes said request to said issuer through said network based on said issuer identification number.

Like claim 1, claim 5 requires a first authorization request from the merchant and a second authorization request from the service provider, the second authorization request transmitted by the service provider including a "second identification number" associated with "the issuer" and "a second payment account number that is not included in the first authorization request". As discussed above with respect to claim 1, these limitations are not shown by Breck.

Claim 5 also requires "a message authentication code being transmitted in said discretionary data field" of a magnetic stripe data structure format. Appellants note that Breck does not show these limitations. Breck does not deal with or describe "message authentication codes," and in particular does not describe "a message authentication code being transmitted in said discretionary data field," which is required by claim 5.

For at least the foregoing reasons, claim 5 and its dependent claims 7-8 are not anticipated by and are patentable over Breck.

Accordingly, the anticipation rejection of these claims should be reversed.

Claims 9-16

The elements of claim 9 include:

"computer generating a message authentication code based on said transaction data; [and]

transmitting track data in standard track image format to said merchant, said track data comprising said computer generated message authentication code and said second account number, wherein said computer generated message authentication code is directly positioned in the discretionary data field of the standard track image format."

The elements of claim 14 include:

"computing a message authentication code based on said data related to said transaction;

placing said message authentication code in a portion of the discretionary data field of a standard payment card magnetic stripe track format to form a track image; and

transmitting said track image, including said message authentication code, over said payment network, without first storing said message authentication code on a magnetic stripe of a payment card."

Claims 9 and 14 include additional features of appellant s' methods for secure payment transactions. In particular, these claims require "computer generating of a message authentication code" (MAC) based on transaction data, which code is then is directly positioned or placed "in the discretionary data field" of a standard payment card track image and then transmitted over the electronic payment network.

Breck does not show this feature of claims 9 and 14. Breck does not describe any standard payment card track image. As noted above in reference to claim 5, Breck does not deal with or describe "message authentication codes." In particular, Breck does not describe positioning and transmitting a computer generated transaction/message authentication code in the discretionary data field of a standard payment card track image.

For at least the foregoing reasons, claims 9 and 14 and their dependent claims 10-13 and 15-16, respectively, are not anticipated by and are patentable over the cited references.

Accordingly, the anticipation rejection of these claims should be reversed.

VIII. CLAIMS APPENDIX

The rejection of the following claims 1-5 and 7-16 is appealed. The following claim 17 has been withdrawn, but is listed for completeness. Claim 6 as indicated is cancelled

1. A method of conducting a transaction using a payment account for payment over a payment network, the method comprising:

(a) receiving by a service provider other than an issuer of the payment account a first authorization request for the authorization of the transaction using a first payment account number, wherein:

(i) the first payment account number has a service provider identification number that is associated with the service provider other than the issuer and is associated with a second payment account number that has an issuer identification number associated with the issuer, said second payment account number not being included in said first authorization request;

(ii) the first authorization request includes a first acquirer code associated with an acquirer; and

(iii) the first authorization request is routable through the payment network to the service provider based on said service provider identification number;

(b) responsive to the first authorization request, transmitting by the service provider a second authorization request for authorization of the transaction using the second payment account number, the second authorization request including a second acquirer code associated with the service provider and being routable through the payment network to the issuer based on said issuer identification number;

(c) receiving from the issuer a response to the second authorization request transmitted by the service provider, the response including the second acquirer code and being routable through the payment network based on that code; and

(d) transmitting from the service-provider to the acquirer a response to the first authorization request received by the service provider based on the response to the second

authorization request received by the service-provider from the issuer, the response to the first authorization request including the first acquirer code and being routable through the payment network based on that code.

2. The method of claim 1, wherein said response to the second authorization request from the issuer further includes said second payment account number, and said response to the first authorization request by the service provider further includes said first payment account number.

3. The method of claim 1, wherein said first authorization request comprises a message authentication code including transaction data, and said request is formatted with a standard track having a plurality of fields including a discretionary field in which said message authentication code is placed.

4. The method of claim 3, wherein said service provider verifies the message authentication code.

5. A method of conducting a transaction with a merchant over a communications network using a first payment account number that is associated with a second payment account number, the method comprising:

(a) generating a message authentication code based on one or more transaction details;

(b) transmitting at least the first payment account number and the message authentication code to the merchant;

(c) requesting by the merchant a first authorization request for payment of the transaction using the first payment account number, said second payment account number not being included in said first authorization request, the request being formatted as if payment were tendered at a point-of-sale terminal with a conventional magnetic-stripe payment card, the format having a track with at least a discretionary data field and said message authentication code being transmitted in said discretionary data field;

(d) responsive to the authorization request for the first payment account number, requesting an authorization for payment of the transaction using the second payment account number; and

(e) accepting or declining the authorization request for the first payment account number based on the response to the authorization request for the second payment account number and the message authentication code,

wherein said first and second payment account numbers include respective service provider and issuer identification numbers, wherein a service provider other than the issuer receives said merchant's request through a payment network based on said service provider identification number, and wherein said service provider generates said request for authorization of payment using the second payment account number and routes said request to said issuer through said network based on said issuer identification number.

6. (cancelled)

7. The method of claim 5, wherein said service provider includes in said request for authorization for payment an acquirer code associated with said service provider, such that said response from said issuer is routed back to said service provider.

8. The method of claim 7, wherein said request by said merchant includes an associated merchant acquirer code, and wherein said service provider generates a message based on said accepting or declining step and routes that message to said associated merchant acquirer code.

9. A method of conducting a transaction over a communications network, the method comprising:

issuing by an issuer having an issuer identification number a first payment account number to a user having a computer, said issuer identification number being associated with said first payment account number;

providing a security module for generating a secret key unique to each first account number issued;

generating a second account number associated with said first payment account number;

providing a secure payment application by a service provider to said computer, said application comprising said second account number and said secret key;

storing said secure payment application on said computer;

selecting a merchant with whom to conduct said financial transaction, said merchant having an associated acquirer code;

passing to said computer transaction data;

computer generating a message authentication code based on said transaction data;

transmitting track data in standard track image format to said merchant, said track data comprising said computer generated message authentication code and said second account number, wherein said computer generated message authentication code is directly positioned in the discretionary data field of the standard track image format;

generating a first authorization request based on said data;

transmitting said first request to said service provider;

verifying said first request with said secret key;

obtaining said first payment account number associated with said second account number;

transmitting a second authorization request using said first payment account number to said issuer identification number associated with said first payment account number; and

authorizing or rejecting said second request.

10. The method of claim 9, wherein said track data comprises a discretionary data field, an account number field, and an expiration date field, and wherein said transmitting track data step further includes

placing said message authentication data in said discretionary data field;

placing said second account number in said account number field; and

placing an expiration date in said expiration date field.

11. The method of claim 10, wherein said transaction data include said associated acquirer code, and a transaction amount.

12. The method of claim 11, wherein said verifying step further includes verifying said transaction data.

13. The method of claim 9, wherein said second authorization request includes a second acquirer code associated with said service provider, and further comprising the steps of:

generating a message based on said authorizing or rejecting step;

forwarding said message to said service provider based on said acquirer code; and

using said merchant's associated acquirer code to advise said merchant of said message.

14. A method of conducting a transaction involving a merchant over an electronic payment network, the method comprising:

receiving data related to said transaction from said merchant;

computing a message authentication code based on said data related to said transaction;

placing said message authentication code in a portion of the discretionary data field of a standard payment card magnetic stripe track format to form a track image; and

transmitting said track image, including said message authentication code, over said payment network, without first storing said message authentication code on a magnetic stripe of a payment card.

15. The method of claim 14, wherein said computing a message authentication code is further based on a transaction sequence number.

16. The method of claim 15, wherein placing said message authentication code in a portion of the discretionary data field further includes inserting at least a portion of said transaction sequence number in a portion of the discretionary data field of said track image, and wherein transmitting said track image further includes transmitting said at least a portion of said transaction sequence number over said payment network.

17. (Withdrawn) An apparatus for conducting a transaction involving a cardholder and merchant having a merchant device over an electronic payment network, the apparatus comprising:

a cardholder memory device;

a cardholder processor capable of executing instructions in a payment application stored in said memory device;

a secret key stored in said cardholder memory device;

said payment application including instructions executable by said cardholder processor to:

receive data related to said transaction from said merchant device;

calculate a message authentication code using at least said data related to said transaction and said secret key; and

transmit at least a portion of said message authentication code to said merchant device for inclusion in a portion of the discretionary data field of track image data formatted as a standard payment card magnetic stripe track data, to be sent over said payment network, without first storing said message authentication code on a magnetic stripe of a payment card.

IX. EVIDENCE APPENDIX

None.

X, RELATED PROCEEDINGS APPENDIX

None.

For the foregoing reasons, the Examiner' rejection of claims 1-5 and 7-16 should be reversed.

Respectfully submitted,

Dated: May 17, 2007

By: _____

Manu J Tejwani
Patent Office Reg. No. 37,952

Attorney for Appellants
Telephone: (212) 408-2614

Baker Botts L.L.P.
30 Rockefeller Plaza
New York, NY 10112